

## **AFFIDAVIT**

I, Aaron M. Miller, a Special Agent with the United States Department of the Treasury, Internal Revenue Service - Criminal Investigation (IRS-CI), being duly sworn, depose as follows:

### **I. INTRODUCTION**

1. I am a Special Agent with the Internal Revenue Service- Criminal Investigation presently assigned to the Toledo, Ohio post of duty, and I have been employed in this capacity since July 2017. As an IRS-CI Special Agent, my duties include, but are not limited to, investigating violations of the Internal Revenue Code, federal laws governing financial crimes and related offenses, and money laundering. Prior to becoming a Special Agent with IRS-CI, I was employed as a Revenue Agent with the Large Business & International (LB&I) division of IRS for approximately ten years. I have a bachelor's degree in accounting and a master's degree specializing in finance.
2. I have completed approximately 26 weeks of law enforcement training at the Federal Law Enforcement Training Center in Glynco, GA. This training covered many aspects of conducting financial investigations, including: a) identifying the means and techniques by which persons engaged in criminal activities derive, launder, conceal, and spend illegally-obtained proceeds and use their businesses and assets to facilitate unlawful activities; b) the preparation of affidavits in tax and non-tax investigations in support of the seizure of financial and tax records, ledgers, books, cash and other valuables, documentation reflecting tax and non-tax violations, and records pertaining to the acquisition and ownership of assets.
3. My duties as an IRS-CI Special Agent involve analyzing records to determine the existence of criminal activity and to develop evidence of criminal activity. My duties as a Special Agent also include conducting financial investigations of individuals and businesses that have violated Federal Law, particularly those laws found under Title 18, Title 26 and Title 31 of the United States Code.
4. I have discussed the facts and evidence of this case with my Supervisory Special Agent and Senior Special Agents who have conducted and participated in multiple investigations involving violations of these statutes. Through these reviews, I have gained a significant amount of insight regarding violations of Title 18, Title 26 and Title 31 of the United States Code. Furthermore, those agents are in agreement about the facts in this case.

5. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Unless otherwise stated, the information in this affidavit is either personally known to me, or has been provided to me by witnesses or other law enforcement officers and/or is based on a review of various documents and records as more particularly described herein.

## II. PLACES TO BE SEARCHED

See Attachment A

6. I submit that evidence, fruits and instrumentalities of the following crimes: Title 26 U.S.C. §7202 (Willful Failure to Collect or Pay Over Tax) and 26 U.S.C. §7206(2) (Aiding or advising preparation or presentation of false return, affidavit, claim, or other document) are located at a residence located in Toledo, Ohio, owned by MICHAEL R. MERIDIETH, JR. (hereinafter referred to as MERIDIETH), as more fully described in Attachment A, which is incorporated herein.
7. Locations to be searched include the person of MERIDIETH, if physically located in the location at the time of the execution of the search warrant for electronic devices and any other material enumerated in Attachment B.

## III. ITEMS TO BE SEIZED

See Attachment B

8. A list of specific items to be seized from the location specified in Attachment A is included in Attachment B, which is incorporated herein.

## IV. PURPOSE OF AFFIDAVIT

9. I am currently investigating MERIDIETH for potential Title 26 violations related to tax years 2013 through 2018. MERIDIETH is the listed owner/operator of Caementum LLC (Caementum) and KDM Group, LLC (KDM) located in Toledo, Ohio. As detailed in this affidavit, MERIDIETH collected payroll withholdings from employees during the years under investigation. However, MERIDIETH willfully failed to pay over employee withholdings and employer taxes to the IRS and instead disposed of the funds on personal purchases primarily through a business credit card and business bank account debit card purchases. As a result of his

actions, MERIDIETH knowingly and intentionally failed to fulfill his legal obligations of collecting, accounting for, and paying over payroll taxes.

10. Additionally, I am currently investigating MERIDIETH for potential Title 26 violations related to tax years 2014-2016. During the period that MERIDIETH and Lonnie Meridieth (Lonnie) owned Caementum together, MERIDIETH volunteered to prepare Lonnie and Stacy Meridieth's (Stacy) personal income tax return. MERIDIETH knowingly and willfully prepared false income tax returns on behalf of Lonnie and Stacy without Lonnie and Stacy's knowledge or authorization.
11. Supported by evidence outlined in this affidavit, I believe there is probable cause to believe MERIDIETH knowingly and willfully failed to pay over employment taxes in violation of 26 U.S.C. §7202 and knowingly and willfully prepared false income tax returns on behalf of Lonnie and Stacy Meridieth in violation of 26 U.S.C. §7206(2).

#### V. AFFIANT'S KNOWLEDGE

Based on my training and experience as a Special Agent, the experience of other Special Agents, and persons knowledgeable in computer forensics, I know:

12. That individuals engaged in an income-producing activity normally maintain financial records, income tax records, property records, and business records in their residences and offices. Financial, property, and business records are also maintained on computers, discs, flash drives, DVD drives, detachable drives, and other electronic devices that store data and are maintained at residences and offices;
13. That individuals engaged in fraud frequently retain records of their transaction within their place of business, or other places under their control. These records may be in the form of written notes and correspondence, receipts, negotiated instruments, contracts, bank statements, and other records. Records of this kind are also often stored on computer media;
14. Persons engaged in fraud often maintain such records for long periods of time, particularly when they are involved in ongoing criminal conduct over a long period of time;
15. There are many reasons why criminal offenders maintain evidence for long periods of time. The evidence may be innocuous at first glance (e.g. financial, credit card and banking documents, travel documents, receipts, documents reflecting purchases of assets, personal calendars, telephone and address directories, check books, videotapes, photographs, utility records,

ownership records, letters and notes, tax returns and financial records, escrow files, telephone and pager bills, keys to safe deposit boxes, packaging materials, computer hardware and software), but have significance and relevance when considered in light of other evidence. The criminal offender may no longer realize he/she still possesses the evidence or may believe law enforcement could not obtain a search warrant to seize the evidence. The criminal offender may also be under the mistaken belief that he/she has deleted, hidden or further destroyed any computer-related evidence, which may be retrievable by a trained forensic computer expert;

16. Owners and operators of businesses maintain records including: invoices, cash receipts journals, loan records, notes, ledgers, bank records, blank forms, contracts, receipts, copies of cashier's checks, copies of money orders, customer lists, and other financial instruments. Business records including books, ledgers, copies of checks, and employee information are maintained where they are most readily accessible, usually on the business premises but sometimes at the residence of the business owner;
17. Owners and operators of businesses maintain safes on the premises in which cash, receipts, and other records are often kept in the ordinary course of business;
18. Frequently it is impossible to directly prove the income of people who have engaged in a pattern of financially deceptive or unrecorded transactions. In those cases, the IRS must resort to a net worth, expenditures or other indirect analysis. To perform that analysis, it is necessary to have the records for a base year immediately preceding the first year in which suspect activities have been identified;
19. Business owner(s) often use computers to record business information and generate business documents including sales data, accounting information, inventory reports, customer lists and the like;
20. As described in Attachment B, this application seeks permission to search for records and other evidence that might be found on the premises described in Attachment A, in whatever form they are found. One form in which the records or other evidence may be found is data stored on a computer's hard drive or other storage media, including cellular telephones. Thus the warrant applied for would authorize the seizure of electronic storage media, or, potentially, the copying of electronically stored information, all under Rule 41 (e)(2)(B);
21. I submit that if a computer or storage medium is found on the premises, there is probable cause to believe records or other evidence will be stored on that computer or storage medium, for the following reasons:

- a. Based on my knowledge, training, and experience, as well as those of other law enforcement officers with knowledge of this investigation, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded onto a storage medium can be stored for years at little or no cost. Even when the files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data;
  - b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space-that is, in space on the storage medium that is not currently being used by an active file for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file;
  - c. Wholly apart from user-generated files, computer storage media-in particular, computers' internal hard drives-contain electronic evidence of how a computer has been used; what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is normally required for that task. However, it is technically possible to delete this information;
  - d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache;"
22. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this electronic evidence will be on any storage medium in the premises because:
- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging

- systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, that attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files created and the sequence in which they were created, although this information can later be falsified;
- b. As examined herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (i.e., registry information, communications, images and motives, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file

data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement);

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when;
- d. The process of identifying the exact electronically stored information on storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant;
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent;

23. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of the premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the

computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine the storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site;
- b. *Technical requirements.* Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge;
- c. *Variety of forms of electronic media.* Records and evidence sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools;
- d. *Nature of examination.* Based on the foregoing, and consistent with Rule 41 (e)(2)(B), the warrant sought would permit seizing, imaging, or otherwise copying storage media that reasonably appears to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant;



24. As described above and in Attachment B, this application seeks permission to search for records that might be found, in whatever form they are found, whether physical or electronic. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e) (2) (B);
25. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output (or I/O) devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating system, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation, and data security devices;
26. Data analysts may use several different techniques to search electronic data for evidence or instrumentalities of crime. These include, but are not limited to, the following: examining file directories and subdirectories for the lists of files they contain; "opening" or reading the first few "pages" of selected files to determine their contents; scanning for deleted or hidden data; and searching for key words or phrases ("string searches");
27. If, after inspecting the I/O devices, software, documentation, and data security devices, the analyst determines that these items are no longer necessary to retrieve and preserve the data evidence, the government will return them within a reasonable time;
28. I submit that this warrant would permit law enforcement to compel certain individuals to unlock a device subject to seizure pursuant to this warrant using the device's biometric features. I seek this authority based on the following:
  - a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition

- features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize;
- b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID. Fingerprint scanners found on devices produced by other manufacturers have different names but operate similarly to Touch ID;
  - c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face;
  - d. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user’s face and activates an infrared-sensitive camera to record data based on patterns within the user’s irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello;

- e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device;
- f. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant;
- g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time;
- h. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device

is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the Subject Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above;

- i. Due to the foregoing, if law enforcement personnel encounter a device that is subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device(s), to the fingerprint scanner of the device(s) found at the premises; (2) hold the device(s) found at the premises in front of the face to those same individuals and activate the facial recognition feature; and/or (3) hold the device(s) found at the premises in front of the face of those same individuals and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

#### VI. INVESTIGATION BACKGROUND

Based on my training and experience as a Special Agent, the training and experience of other Special Agents, I know and/or have been advised of the following:

29. This investigation indicates alleged violations of Title 26, United States Code, Section 7202 (Willful Failure to Collect or Pay Over Tax), with respect to federal business employment tax returns submitted to the IRS by MERIDIETH for tax years 2013 to 2018. This section provides that “[a]ny person required under this title to collect, account for, and pay over any tax imposed by this title who willfully fails to collect or truthfully account for and pay over such tax shall, in addition to other penalties provided by law, be guilty of a felony and, upon conviction thereof, shall be fined not more than \$10,000, or imprisoned not more than 5 years, or both, together with the costs of prosecution.”

30. This investigation also indicates alleged violations of Title 26, United States Code, Section 7206(2) (Aiding or advising preparation or presentation of false return, affidavit, claim, or other document), with respect to federal personal income tax returns prepared by MERIDIETH and submitted to the IRS by Lonnie and Stacy for tax years 2013 to 2016. This section provides that “[a]ny person who... willfully aids or assists in, or procures, counsels, or advises the preparation or presentation under, or in connection with any matter arising under, the internal revenue laws, of a return, affidavit, claim, or other document, which is fraudulent or is false as to any material matter, whether or not such falsity or fraud is with the knowledge or consent of the person authorized or required to present such return, affidavit, claim, or document;... shall be guilty of a felony and, upon conviction thereof, shall be fined not more than \$100,000 (\$500,000 in the case of a corporation), or imprisoned not more than 3 years, or both, together with the costs of prosecution.”
31. MERIDIETH's father, Michael Meridieth Sr., who is now deceased, and Lonnie were brothers and had previously owned and operated Meridieth Construction, Inc., a concrete construction business. Lonnie and Michael Meridieth Sr. started Meridieth Construction, Inc. in 1993. Lonnie's responsibility and job description was construction field management and supervision, supervising all job sites in the field, and Michael Meridieth Sr. was responsible for securing contracts and running the office. Due to health reasons, Lonnie bought out his brother Michael in 2002 and operated Meridieth Construction, Inc. as sole owner until the business was closed in 2008.
32. Once Meridieth Construction, Inc. closed, Lonnie Meridieth went to work for Keystone Foundation Systems as a Form W-2 wage earning employee. Lonnie had the title Concrete Superintendent and had similar responsibilities as when he owned Meridieth Construction, Inc.
33. After being bought out by his brother, Michael Meridieth Sr. and MERIDIETH started Meridieth Concrete, LLC, a concrete construction business, on March 5, 2002, per State of Ohio business filings. Michael Meridieth Sr. passed away in 2004 and MERIDIETH continued to operate Meridieth Concrete, LLC. IRS Small Business / Self Employed Collection Division conducted lien and levy actions against the business and, according to State of Ohio business filings filed by MERIDIETH on November 8, 2011, Meridieth Concrete, LLC ceased operations on May 31, 2008.

34. MERIDIETH formed Allied Construction Services, LLC, a concrete construction business, April 16, 2008 according to State of Ohio business filings. MERIDIETH operated Allied Construction Services, LLC until early 2009, at which time IRS Small Business / Self Employed Collection Division conducted lien and levy actions against the business. State of Ohio business filings filed by MERIDIETH on November 8, 2011, show Allied Construction Services, LLC ceased operations on March 31, 2009.
35. MERIDIETH formed Interlock Construction Services, LLC, a concrete construction business, June 25, 2010 according to State of Ohio business filings. MERIDIETH operated Interlock Construction Services, LLC until mid-2011 when IRS Small Business / Self Employed Collection Division conducted lien and levy actions against the business. State of Ohio business filings filed by MERIDIETH on November 8, 2011, show Interlock Construction Services, LLC ceased operations on August 1, 2011.
36. After the closure of Interlock Construction Services, LLC, MERIDIETH approached Lonnie about working for him at Keystone Foundation Systems because MERIDIETH needed health insurance. Lonnie was able to get MERIDIETH a job working for him at Keystone Foundation Systems.
37. While at Keystone, MERIDIETH began to secure side contracting jobs and eventually approached Lonnie about going into business together. MERIDIETH asked Lonnie to perform concrete construction field management and supervision as he had with MERIDIETH's father. MERIDIETH asked Stacy to complete formation of Caementum with the State of Ohio, obtain a Federal ID number, and open a bank account at Huntington for the business as a convenience. On March 2, 2012, Stacy filed organization documents for Caementum with the State of Ohio.
38. IRS Small Business / Self Employed Collection Division conducted lien and levy actions against Caementum when Lonnie states Caementum ceased operations in January or February, 2018.
39. MERIDIETH formed KDM on May 5, 2011 according to State of Ohio business filings. Meridieth began using KDM as a concrete construction business in the summer, 2018, but KDM was reported on MERIDIETH's Schedule C as a consulting business for all tax years under investigation. MERIDIETH continues to own and operate KDM as of the date of this affidavit.
40. A Schedule C is a form attached to a Form 1040, U. S. Individual Income Tax Return (Form 1040), personal tax return, which is used to report self-employment business income. Unless the

self-employment business income was reported by a third party to the IRS on a Form 1099, it can be difficult or even impossible to verify reported Schedule C income.

41. Owners of sole proprietorships commonly report business income and related expenses on the owner's personal income tax return. Page 1 of an individual's tax return generally shows all the different types of income an individual can report, including Schedule C business income. A business owner who files one or more Schedule Cs (Profit or Loss From Business) will report the combined net income from all Schedule C business activity on Line 12 on Page 1 of the Form 1040.
42. A Subchapter S corporation, also known as an S corp, is a specific type of corporation; the other type is a Subchapter C corporation. An S corp provides all the advantages of a corporate business structure while allowing the profits and losses to pass through to the shareholder(s), just as in an LLC or partnership. A corporation is a form of business that is owned by its shareholder(s) and which assumes liability for the actions and finances of the business – the shareholders cannot be held responsible. Being able to shift liability away from the owner and onto the business itself is a major advantage.
43. A Form 1120-S is an income tax return prepared for and filed by an S corp. An S corp is a closely held corporation that makes a valid election to be taxed under Subchapter S of Chapter 1 of the Internal Revenue Code. In general, S corps do not pay any federal income taxes. Instead, the corporation's income or losses are divided among and passed through to its shareholders.
44. An S corp annually prepares and files a Form 1120-S with the IRS. Similar to a Form 1065 for a partnership, a Form 1120-S reports the reportable income and associated business expenses of the S corporation and determines each shareholder's pro rata share items. Each shareholder's pro rata share items are reported to the IRS and disclosed to the shareholder via a Schedule K-1, Shareholder's Share of Income, Deduction, Credits, etc.
45. A shareholder reports the Schedule K-1 information on Schedule E (Supplemental Income and Loss from... S Corporation...) of the Form 1040. All rental real estate, royalties, partnerships, S corporations, estates, and trusts activities are combined and reported as one net income number on Line 17 on Page 1 of Form 1040.
46. For the 2013 through 2016 tax years, Caementum reported income and expenses on a Schedule C for tax reporting purposes on Lonnie and Stacy's joint Forms 1040. Lonnie and Stacy's 2017 Form 1040 does not have a Schedule C included.



47. On MERIDIETH's 2017 Form 1040, 50% of Caementum's losses for the year are reported on the Schedule E stating Caementum is operating as an S corp. However, there are no filings on record with the IRS for a Form 1120-S for 2017 for Caementum and there is no indication as to who is reporting the other 50% of the operating loss. Lonnie and Stacy do not have a Schedule E included on their 2017 Form 1040.

## VII. SUMMARY OF PROBABLE CAUSE

48. IRS records show that Caementum, as of the date of this affidavit, owes \$ 935,266.00 to the Department of the Treasury for unpaid Employer Taxes, Unemployment Taxes and Employee withholdings.
49. A criminal investigation of MERIDIETH was initiated following a fraud referral from IRS, Small Business / Self Employed.
50. Revenue Officer Janet Kimple (RO Kimple) was the IRS Revenue Officer assigned to the case. A typical IRS collection case involves an IRS Revenue Officer interviewing taxpayers and employees of their businesses, reviewing and analyzing business records, and making attempts to voluntarily or involuntarily collect on taxes due and owing to the Department of the Treasury.
51. RO Kimple stated that Caementum is the fourth business MERIDIETH has owned, all of which have had IRS Small Business / Self Employed Collection Division levy and lien actions brought against them. MERIDIETH has been assessed trust fund recovery penalties for Meridieth Concrete, Allied Construction Services, Interlock Construction, and Caementum. RO Kimple received substantial amounts of banks records and, after reviewing bank records and interviewing MERIDIETH, Lonnie and Stacy, determined that the records and testimony reveal a significant misuse of company funds, including support of a personally lavish lifestyle, while employment taxes went unpaid. These records, along with learning that MERIDIETH was now operating a fifth business, KDM, are the basis for RO Kimple's fraud referral to IRS-CI.
52. In June, 2018, independent of the fraud referral, Lonnie and Stacy submitted a Statement of Facts to IRS-CI through their attorney, Gary Harden, reflecting the statement of Lonnie and Stacy on this matter.
53. I interviewed Stacy on July 25, 2019. During the interview, Stacy stated the following:



- a. Stacy confirmed the Statement of Facts previously provided to IRS-CI through her attorney is Lonnie and Stacy's statement. There is no additional information Stacy needs to add to the Statement of Facts since it was originally received by the IRS in June 2018.
- b. Lonnie and Stacy found out that MERIDIETH was operating another business at Lonnie's brother's funeral in May, 2019. Stacy verified the business existed by driving to the office at the intersection of Lewis and Laskey in Toledo, OH. Stacy noticed a sign on the window stating "KDM Group" and noticed MERIDIETH's truck at the location.
- c. Stacy and Lonnie have "dished out a lot of money to protect ourselves from someone who defrauded us," while MERIDIETH buys snow mobiles, a new truck, new (Ford) Expedition, fleet of trucks for his business (shows jobs on Facebook under "Mike Meridieth" and KDM), snow mobiling trips to Montana, and went to South Carolina with his wife, visiting a fancy steakhouse called Ruth's Chris.
- d. Stacy explained that, with very limited exception, all expenses charged to Capital One Spark Business business credit card account # ending in 0999 were personal in nature.
- e. Stacy was aware that the business bank account was used to pay personal expenses.

54. I interviewed Lonnie on July 25, 2019. During the interview, Lonnie stated the following:

- a. Lonnie confirmed the Statement of Facts previously provided to IRS-CI through his attorney is Lonnie and Stacy's statement, which he reviewed the week prior to our interview, and there is no additional information Lonnie needs to add to the Statement of Facts since it was received by the IRS in June 2018.
- b. All the books and records have been and still are in MERIDIETH's possession. While MERIDIETH was in rehab in 2015, Lonnie went to MERIDIETH's house and used the business computer to pay employees.
- c. Lonnie understood that he and MERIDIETH were 50/50 partners in the LLC. Lonnie did not understand that, while they received the same amount of compensation, MERIDIETH would direct his full compensation to a separate limited liability company while Lonnie received a regular paycheck net of withholdings and deductions.
- d. Caementum only had construction projects in Ohio and Michigan.
- e. Lonnie used the business debit card and credit card for personal expenditures and was aware funds from the business checking account were paying those expenses.

55. I interviewed Lonnie again on August 5, 2019. During the interview, Lonnie stated the following:

- a. MERIDIETH lives on Fredelia Drive in Sylvania Township.
- b. MERIDIETH kept all Caementum's records at his house. MERIDIETH had file cabinets, a desk with papers and also kept blue prints of job sites.
- c. While reviewing Lonnie and Stacy's 2014 Form 1040:
  - i. MERIDIETH prepared the Form 1040, it was not "self-prepared."
  - ii. Lonnie did not authorize MERIDIETH to include all the business income on his personal Form 1040.
  - iii. Lonnie did not have unreimbursed business expenses and did not authorize MERIDIETH to include \$17,666 of expenses on his return.
  - iv. Lonnie did not authorize MERIDIETH to deduct Lonnie's personal residence as a business expense on Lonnie's Form 1040.
- d. While reviewing Lonnie and Stacy's 2015 Form 1040:
  - i. MERIDIETH prepared the Form 1040, it was not "self-prepared."
  - ii. Lonnie did not authorize MERIDIETH to exclude Lonnie's W-2 wages from Lonnie's Form 1040.
  - iii. Lonnie did not authorize MERIDIETH to include \$3.1 million in business income on Lonnie's Form 1040, Schedule C.
  - iv. Lonnie did not authorize MERIDIETH to exclude self-employment taxes from Lonnie's Form 1040.
  - v. Lonnie stated unreimbursed business expenses totaling \$25,840 is false and Lonnie has no idea where that number came from
- e. While reviewing Lonnie and Stacy's 2016 Form 1040:
  - i. MERIDIETH prepared the Form 1040, it was not "self-prepared."
  - ii. Lonnie did not authorize MERIDIETH to include \$3.4 million in business income on Lonnie's Form 1040, Schedule C.
  - iii. Lonnie does not know how a \$190,000 loss on Lonnie's Form 1040, Schedule C was calculated.
- f. Lonnie did not authorize MERIDIETH to put business activity on Lonnie's Form 1040.

- g. MERIDIETH was in charge of all the accounting and kept all the business records at MERIDIETH's house. Lonnie provided MERIDIETH with Lonnie and Stacy's Form W-2 and charitable deduction information for MERIDIETH to prepare Lonnie and Stacy's Form 1040. All business data used to prepare Lonnie and Stacy's Form 1040s are in MERIDIETH's possession.
56. A statement signed by MERIDIETH on June 5, 2018, was provided to the IRS Small Business / Self-Employed Collection Division by Gary Harden, Lonnie and Stacy's attorney. The statement was prepared as a result of Lonnie and Stacy's IRS appeals hearing to protest the assessed trust fund recovery penalty against Lonnie and Stacy. Gary Harden confirmed the statement during my interview with Stacy on July 25, 2019. In the statement submitted by MERIDIETH, MERIDIETH admitted that he maintains books, accounts, and other records at his home office.
57. Lucas County, Ohio, real estate records show MERIDIETH purchased his current home on Fredelia Drive on April 28, 2017.

**Analysis of Form 1040, U.S. Individual Income Tax Returns (Forms 1040) and  
Form 941, Employer's Quarterly Federal Tax Returns (Form 941)**

58. IRS records show for tax years 2012 through 2016, MERIDIETH (XXX-XX-4900) filed Forms 1040, with the filing status of "head of household". IRS records show for the 2017 tax year, MERIDIETH's filed a Form 1040 with the filing status of "married filing separate." As of the date of this affidavit, MERIDIETH's 2018 individual income tax return was on extension and had not yet been received and processed by the IRS.
59. A home address of 5329 Fredelia Drive, Toledo, OH 43623 was listed on MERIDIETH'S 2016 and 2017 Forms 1040 as well as MERIDIETH's 2018 Form 4868 (Application for Automatic Extension of Time to File U.S. Individual Income Tax Return).
60. IRS records show that for tax years 2012 through 2018, Lonnie (XXX-XX-8195) and Stacy (XXX-XX-8879) filed Forms 1040, with the filing status of "married filing jointly".
61. IRS records show that Lonnie and Stacy reported all Caementum's income and expenses on a Schedule C, Profit or Loss from Business under the business name "Caementum LLC" for the years 2013 through 2016. Stacy is listed as the proprietor and a business address listed is the same as Lonnie and Stacy's personal residence at 5045 Courville Avenue, Toledo, Ohio 43623.
62. For 2017, IRS records show that MERIDIETH reported Caementum as being an S corp by

reporting a Schedule K-1 from Caementum on his Schedule E. However, IRS records do not show a Form 1120-S filed for Caementum for 2017, Lonnie and Stacy did not report a Schedule K-1 on their Schedule E, and Lonnie and Stacy MERIDIETH did not report any Caementum income or expenses on a Schedule C.

63. IRS records show that Caementum did not timely file Forms 941, Employer's Quarterly Federal Tax Return. Caementum was audited by an employment tax specialist for the IRS Small Business / Self Employed division. During the audit, the examiner prepared and filed a "Substitute for Return," a process by which the IRS examiner prepares a tax return based on information return information available and posts the return to the individual or business's tax module. The substitute for return process was completed for the 2013 through 2015 employment tax years. MERIDIETH prepared and filed Forms 944, Employer's Annual Federal Tax Return for 2016 and 2017.
64. IRS records show that KDM began employing workers during the third quarter (July – September) of 2018. KDM has filed Form 941s, Employer's Quarterly Federal Tax Return, for the third and fourth quarters of 2018 and the first quarter 2019. IRS records show that only one of the three quarters was paid in full, leaving a balance due for the quarters ending September 2018 and March 2019. Second quarter 2019 (April – June) is due July 31<sup>st</sup> and has not yet been filed as of August 13, 2019.
65. IRS records show that a CP 276B Notice (Did Not Receive Timely Tax Deposits) and a CP 134B Notice (Form 941 Balance Due) were issued to "KDM Group LLC Michael R Meridieth Sole Mbr" at the address of "1055 Custer Drive, Toledo, OH 43612" the week of May 12, 2019. IRS records also show that a CP 504B Final Notice (Notice of Intent to Levy) was issued to "KDM Group LLC Michael R Meridieth Sole Mbr" at the address of "1055 Custer Drive, Toledo, OH 43612" the week of June 16, 2019 for a Form 941 balance due totaling \$2,033.62.

#### **Review of Bank Accounts and Credit Cards of**

#### **Caementum LLC, KDM Group LLC, MICHAEL, Lonnie, & Stacy MERIDIETH**

66. Account # ending in 8693 is Caementum's business checking account at Huntington National Bank. The signature card lists "Caementum LLC 5045 Courville Ave, Toledo OH 43623-2922" as the account holder and street location. The signature card was updated eight (8) times between June, 2012 and November 2015 with the most current signature card dated 11/23/2015. Stacy

was an authorized signer on all eight signature cards, MERIDIETH was an authorized signer on five signature cards, and Lonnie was an authorized signer on two signature cards.

67. Account # ending in 0412 is MERIDIETH and Kristin Childress's (MERIDIETH's spouse) checking account at Huntington National Bank. The signature card lists "Michael R Meridieth" as the primary owner and "Kristin Childress" as the additional owner. This signature card does not list an address for the account owner. The signature card was last updated on 2/3/2016. Account Bank Statements starting 4/14/2017 through the end of 2018 lists "Michael R Meridieth Kristin Childress 5329 Fredelia Dr, Toledo, OH 43623-1561" as the account holder and street location.
68. Account # ending in 2256 is Caementum's business checking account at Citizens Bank. The signature card lists "Caementum LLC 715 Spencer St Toledo, OH 43609" as the account holder and street location. MERIDIETH is the sole authorized signer on the account. The signature card was last updated on 2/24/2018, when the business checking account was opened.
69. Account # ending in 2248 is KDM's business checking account at Citizens Bank. The signature card lists "KDM Group LLC 5329 Fredelia Dr Toledo, OH 43623-1561" as the account holder and street location. MERIDIETH is the sole authorized signer on the account. The signature card was last updated on 2/24/2018, when the business checking account was opened.
70. Account # ending in 0999 is a Capital One Spark Business business credit card. The account is held by "Stacy Meridieth Caementum LLC 5045 Courville Ave Toledo, OH 43623-2922." There are three credit cards issued on this account. The first, ending in 0999, issued to Stacy. The remaining two, ending in 4650 and 9945, issued to Lonnie. Through March, 2017, Stacy incurred all but two credit card transactions and Stacy initiated electronic credit card payments totaling \$13,428 from the LLC's Huntington Bank Checking Account ending in 8693.
71. Account # ending in 4156 is a Capital One Spark Business business credit card. The account is held by "Michael R Meridieth Caementum LLC 2808 Heysler Rd Toledo, OH 43617-1536." There are multiple credit cards issued on this account including one to MERIDIETH ending in 4156, one to Lonnie ending in 0971, and one to Stacy ending in 4675. The remaining cards were issued to Caementum employees and the number of credit cards outstanding varied over the years of credit card statements.

**Analysis of Financial Information**

Credit card statements for Caementum's Capital One Spark Business card accounts ending in 0999 and 4156 were reviewed. The following payments totals were initiated from various bank accounts by MERIDIETH and/or Stacy electronically via Capital One's website or the mobile application:

<b>Initiator</b>	<b>Total</b>	<b>Start Date</b>	<b>End Date</b>	<b>Account Owner</b>	<b>Account Number Ending</b>	
S. Meridieth	13,428.24	12/11/2015	03/16/2017	Caementum LLC	8693	
M. Meridieth	850,673.55	09/22/2014	02/08/2018	Caementum LLC	8693	
M. Meridieth	12,500.00	03/05/2018	06/25/2018	Caementum LLC	2256	
M. Meridieth	42,907.01	04/03/2018	09/10/2018	M. MERIDIETH	0412	
M. Meridieth	110,707.60	06/27/2018	Current	KDM Group LLC	2248	
<b>Total</b>	<b>1,030,216.40</b>					

72. Caementum LLC account # ending in 8693 at Huntington National Bank maintained an average monthly balance of \$84,520 from January, 2013 until the first IRS levy was processed January 23, 2018. The account ending balance peaked at \$266,773 in June, 2016.
73. I observed charges while reviewing the Capital One **business** credit card ending in 0999 totaling \$15,158.07 incurred by Stacy. Stacy caused payments from the Huntington Bank **business** checking account (ending in 8693) totaling \$13,428.24 to be paid toward the outstanding balance on the above referenced Capital One business credit card.
74. I observed charges while reviewing the Capital One **business** credit card ending in 4156 totaling \$41,984.85 incurred by Stacy. MERIDIETH caused payments from the Huntington Bank **business** checking account (ending in 8693) totaling \$850,673.55 to be paid toward the outstanding balance on the above referenced Capital One business credit card.

75. I observed the following expenses while reviewing **business** bank statements for account ending in 8693 at Huntington Bank (expenses over \$1,000 highlighted):

Date of Transaction	Amount of Transaction	Vendor	Location
<b>02/04/2013</b>	<b>\$ 14,932.50</b>	<b>White Star Snowmobile Auction</b>	<b>Bronson, MI</b>
05/28/2013	\$ 974.04	Del Frisco's	Charlotte, NC
<b>06/10/2013</b>	<b>\$ 1,149.99</b>	<b>Safety Services</b>	<b>Tempe, AZ</b>
07/05/2013	\$ 286.25	Kings Point Marina	Cornelius, NC
09/20/2013	\$ 973.40	Airtran Airline Tickets	Atlanta, GA
01/02/2014	\$ 692.62	Big Time Boots	Nashville, TN
01/06/2014	\$ 204.08	Margaritaville	Nashville, TN
01/27/2014	\$ 653.00	U.S. Airways	Las Vegas, NV
02/03/2014	\$ 470.75	Bird's Nest	Chicago, IL
02/03/2014	\$ 534.16	Chicago Cut Steakhouse	Chicago, IL
03/10/2014	\$ 250.33	Plantation House	Lahaina, HI
<b>03/12/2014</b>	<b>\$ 1,208.33</b>	<b>Louis Vuitton</b>	<b>Lahaina, HI</b>
07/14/2014	\$ 399.00	Wolve's Tournament	Livonia, MI
08/22/2014	\$ 653.40	American Airlines	New York, NY
<b>08/28/2014</b>	<b>\$ 2,620.00</b>	<b>Ohio Attorney General</b>	<b>Columbus, OH</b>
09/02/2014	\$ 458.44	131 Main Lake	Cornelius, NC
<b>10/20/2014</b>	<b>\$ 3,297.56</b>	<b>Verizon Wireless</b>	<b>Georgia</b>
12/31/2014	\$ 403.20	Table 26	West Palm Beach, FL
<b>01/29/2015</b>	<b>\$ 6,464.89</b>	<b>Aurhaus Furniture</b>	<b>Perrysburg, OH</b>
03/30/2015	\$ 399.63	Portobello Cucina	Jupiter, FL
<b>06/29/2015</b>	<b>\$ 5,394.89</b>	<b>Jeffrey Mann Fine Jewelers</b>	<b>Toledo, OH</b>
<b>07/14/2015</b>	<b>\$ 1,509.13</b>	<b>McCamly Plaza Hotel</b>	<b>Battle Creek, MI</b>
<b>10/05/2015</b>	<b>\$ 5,761.06</b>	<b>Omni Grove Park Inn</b>	<b>Asheville, NC</b>
10/13/2015	\$ 404.00	Dave & Busters	Livonia, MI
11/09/2015	\$ 350.86	Diplomat Golf & Tennis Club	Hollandale, FL
11/09/2015	\$ 780.00	Miami Gardens	Miami Gardens, FL
12/31/2015	\$ 866.88	Vic & Angelo's PGA	Palm Beach, FL
<b>01/04/2016</b>	<b>\$ 12,656.40</b>	<b>Ballenisses Country Club</b>	<b>Palm Beach, FL</b>
<b>12/07/2016</b>	<b>\$ 3,616.21</b>	<b>Sheraton Vacation Club (Timeshare)</b>	<b>Orlando, FL</b>
Various	\$ 4,037.20	Delta Airlines	Norwalk, CT
Various	\$ 1,280.48	Hilton Nashville	Nashville, TN
Various	\$ 6,117.11	PGA National Resort	Palm Beach, FL
Various	\$ 2,516.14	Ruth's Chris Steak House	Charlotte, NC
Various	\$ 1,379.20	Southwest Airlines	Texas
Various	\$ 20,212.44	The Venue	Asheville, NC
<b>Total</b>	<b>\$ 103,907.57</b>		

76. I observed charges incurred by MERIDIETH and Lonnie while reviewing Capital One **business** credit card account ending in 4156 between April, 2015, and December, 2015, totaling \$64,097.80 summarized below (charges over \$1,000 highlighted):

Date of Transaction	Amount of Transaction	Vendor	Location
04/09/2015	\$ 415.42	Navient Private Credit	Pennsylvania
05/03/2015	\$ 481.49	Hilton Garden Inn	Perrysburg, OH
<b>05/20/2015</b>	<b>\$ 1,558.00</b>	<b>Toledo Door and Window</b>	<b>Toledo, OH</b>
05/24/2015	\$ 206.03	Boulder Creek Golf Club	Streetsborough, OH
<b>06/08/2015</b>	<b>\$ 1,862.62</b>	<b>Radisson Hotel</b>	<b>Chicago, IL</b>
06/08/2015	\$ 559.28	Team Sports	Holland, OH
06/11/2015	\$ 605.00	Miami Gardens Square	Miami, FL
06/19/2015	\$ 857.43	Shanghai Resort	La Follette, TN
06/19/2015	\$ 491.63	Springs Dock Resort	La Follette, TN
07/02/2015	\$ 600.00	McCamly Plaza Hotel	Battle Creek, MI
07/02/2015	\$ 354.70	U.S. Airways (Stacy)	
07/03/2015	\$ 392.00	The Peninsula Club	Cornelius, NC
07/04/2015	\$ 999.98	Lake Norman Marina	Sherrills Ford, NC
07/31/2015	\$ 574.05	Commodore Resorts	Put-In-Bay, OH
<b>08/08/2015</b>	<b>\$ 1,103.32</b>	<b>Beef N Bottles Restaurant</b>	<b>Charlotte, NC</b>
08/22/2015	\$ 307.71	Kalahari Resort	Sandusky, OH
08/28/2015	\$ 462.55	Arizona Grand Resort	Phoenix, AZ
08/31/2015	\$ 358.00	Parker & Sons	Phoenix, AZ
10/01/2015	\$ 568.81	Luella's Bar-B-Que	Asheville, NC
<b>10/01/2015</b>	<b>\$ 2,892.65</b>	<b>Omni Grove Park Golf Course</b>	<b>Asheville, NC</b>
10/04/2015	\$ 692.60	United Airlines (Michael)	Texas
<b>11/08/2015</b>	<b>\$ 1,185.96</b>	<b>Whiskey Tango All American</b>	<b>Hollywood, FL</b>
<b>11/09/2015</b>	<b>\$ 4,455.77</b>	<b>Marriott Hollywood Beach</b>	<b>Hollywood, FL</b>
11/09/2015	\$ 418.71	Royal Rent A Car	Fort Lauderdale, FL
12/01/2015	\$ 752.36	Spirit Airlines (Michael)	Miramar, FL
<b>12/02/2015</b>	<b>\$ 1,178.45</b>	<b>Enterprise Rent-A-Car</b>	<b>Forest Lake, MN</b>
12/02/2015	\$ 577.74	Expedia.com	Nevada
12/21/2015	\$ 252.15	Sports Authority	Palm Beach, FL
<b>01/01/2016</b>	<b>\$ 2,155.94</b>	<b>Seminole Hard Rock Hotel</b>	<b>Fort Lauderdale, FL</b>
Various	\$ 1,546.00	American Airlines (Michael, Lonnie &	Dallas, TX
Various	\$ 1,426.40	Delta Air (Lonnie & Stacy)	
Various	\$ 14,857.56	Hazeldon Serenity Corner	Center City, MN
Various	\$ 9,183.00	HSG Foods	Toledo, OH
Various	\$ 7,279.12	PGA National Golf Resort & Spa	Palm Beach, FL
Various	\$ 2,485.37	Verizon Wireless	Georgia
<b>Total</b>	<b>\$ 64,097.80</b>		



**Summary of Surveillance Activity**

77. On April 26, 2019, I surveilled 1055 Custer Avenue, Toledo, Ohio. I observed “KDM Group LLC” printed on the front window of the office. Two vehicles were observed parked in front of the office. A black Cadillac was registered to Employee 1. A green Lincoln Aviator was registered to the spouse of Employee 2. Employee 1 and Employee 2 were identified as employees through Forms W-2 filed with the IRS by KDM Group LLC and Caementum LLC.
78. On July 8, 2019, I surveilled 1055 Custer Avenue, Toledo, Ohio. I observed that lettering on the front window previously stating, “KDM Group LLC” had been removed and the office space was empty. There were no vehicles parked in front or behind the office space.
79. On July 8, 2019, I surveilled 5329 Fredelia Drive, Toledo, Ohio, the residence of MERIDIETH. I observed a Ford F-250 registered to MERIDIETH parked in the driveway.
80. As of the date of this affidavit, a Google search for “KDM Group Ohio” did not provide a more current address for KDM. KDM’s Facebook page still lists 1055 Custer Avenue, Toledo, Ohio, as the business location. MERIDIETH’s LinkedIn profile states that KDM is located at 1055 Custer Rd., Toledo, OH from April 2011 through the present. LexisNexis Accurint provided 1055 Custer Dr., Toledo, OH and 5329 Fredelia Dr., Toledo, OH as business addresses for KDM.

VIII. CONCLUSION

81. Based on my experience as a Special Agent, that of senior agents with whom I have conferred, and the facts and circumstances presented in this affidavit, it is my opinion that:

- a. there is probable cause to believe MICHAEL R. MERIDIETH, JR. failed to collect or pay over taxes in violation of 26 U.S.C. §7202;
- b. there is probable cause to believe MICHAEL R. MERIDIETH, JR. falsely prepared income tax returns on behalf of Lonnie and Stacy Meridieth in violation of 26 U.S.C. §7206(2);
- c. There is probable cause to believe fruits, evidence, and instrumentalities of said crimes, as detailed in Attachment B, are currently located at the following property which is more fully described in Attachment A: 5329 Fredelia Drive, Toledo, Ohio.

82. I further request that this affidavit and any related applications issued are sealed by this Court. It is my belief that disclosure at this time may jeopardize the ongoing investigation into the above described criminal activity.

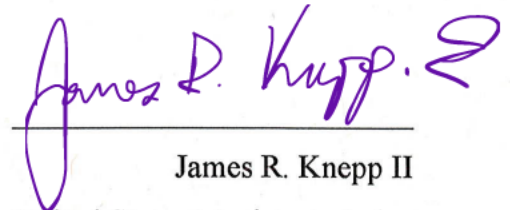


Aaron M. Miller

Special Agent, IRS-CI

Sworn to via telephone after submission by reliable  
electronic means, Fed R. Crim P. 4.1 and 41(d)(3),

this 19th day of September, 2019



James R. Knepp II

United States Magistrate Judge

Toledo, Ohio